### I. PURPOSE

This directive establishes guidelines and responsibilities of Department members using social media outlets.

## II. SCOPE

For the purposes of this directive, the term "social media outlets" means any electronic communication (such as personal Web sites and outlets for social networking and microblogging) through which participants utilize online communities to share information, ideas, personal messages, and other content through an electronic format. These formats include, but are not limited to, text, video, photographs, audio, digital documents, etc.

This directive addresses the full breadth and scope of social media rather than any one particular format. The Department recognizes that as technology advances, new methods for social media participation will emerge.

## III. POLICY

Social media outlets, when used in a proper manner, can reinforce the Department's relationship with the public, build community support, and assist in solving crime. Department members have a constitutional right to express their views under the First Amendment. However, Department members may be subject to discipline for violating the provisions of this directive. Any social media participation made pursuant to a Department member's official duties is not considered protected speech under the First Amendment.

# IV. DEPARTMENT SOCIAL MEDIA OUTLETS

#### A. Procedures

- 1. All Department social media outlets shall be approved by the Superintendent or his/her designee and shall be administered by Public Safety Information Technology (PSIT).
- 2. The use of Department computers by Department members to access any social media outlet is prohibited absent prior supervisory approval.
- 3. Social media content shall adhere to applicable laws, the <u>Rules and Regulations of the Chicago Police Department</u>, and any relevant Department policies, including all information technology and records management policies.
  - a. Department records retention schedules shall apply to social media content.
  - b. Content is subject to Local Records Act (50 ILCS 205/1).
  - c. Content must be managed, stored, and retrievable in compliance with the Illinois Freedom of Information Act (<u>5 ILCS 140/1</u>) and any relevant Department directives.
- B. Department members authorized to administer Department social media outlets shall:
  - 1. conduct themselves at all times as representatives of the Department and, accordingly, shall adhere to applicable Department Rules and Regulations and Department directives.
  - 2. not make statements indicating the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions.

- 3. not post, transmit, or otherwise disseminate confidential information related to Department training, activities, or on-going investigations without express written permission.
- 4. comply with all copyright, trademark, and service mark restrictions in posting materials to electronic media.
- 5. not use personally owned devices to manage the Department's social media activities without proper approval.
- 6. ensure that all relevant privacy protections are maintained.

## V. DEPARTMENT MEMBERS' PERSONAL USE OF SOCIAL MEDIA OUTLETS

- A. When using social media, Department members should be mindful that their communications become part of the worldwide electronic public domain. Department members should be aware that privacy settings and social media sites are subject to constant modifications, and they should never assume that personal information posted on such sites is protected or secure.
- B. Department members should expect that any information that they create, transmit, download, exchange, or discuss that is available online in a public forum may be accessed by the Department without prior notice.
- C. Department members are prohibited from posting, displaying, or transmitting:
  - 1. any communications that discredit or reflect poorly on the Department, its missions or goals.
  - 2. content that is disparaging to a person or group based on race, religion, sexual orientation, or any other protected class.
  - 3. Department information, records, documents, video recordings, audio recordings, or photographs to which they have access as a result of their employment without the written permission from the Office of News Affairs or the Office of the Superintendent.
  - 4. any references to any other Department member's employment by the Department without that person's consent.
  - 5. any intellectual property of the Department or the City of Chicago without the specific authorization of the Superintendent or his/her designee. Department or City of Chicago intellectual property includes but is not limited to logos, uniforms, official photographs, audio/ video files, or any text documents (paper or electronic).
  - 6. <u>any information representing themselves as an official spokesperson of the Department and the City of Chicago unless specifically authorized by the Superintendent or his/her designee.</u>

## VI. USE OF SOCIAL MEDIA OUTLETS FOR INVESTIGATIVE PURPOSES

- A. Social media is a valuable investigative tool when seeking evidence or information about:
  - 1. missing persons;
  - 2. wanted persons;
  - 3. gang participation and retaliation;
  - 4. crimes perpetrated online (i.e., cyberbullying, cyberstalking); and
  - 5. photos or videos of a crime posted by a participant or observer.
- B. Department members utilizing a social media outlet as an investigative tool will:
  - use only Department electronic equipment throughout the investigation.
  - 2. conduct an investigation only while on duty.
  - 3. <u>follow the guidelines set forth in the Rules and Regulations of the Chicago Police Department and the Department directives including, but not limited to, "Use of the Internet" and "Department-Issued Electronic Communication Devices."</u>
  - 4. only use publicly available open source material.

- C. Department members utilizing a social media outlet as an investigative tool will not:
  - 1. <u>use their personal social media account or personal account information to access the social media content.</u>
  - 2. <u>use another individual's personal account without his/her consent and the approval of their</u> Bureau Chief.
  - 3. <u>actively participate in any discussion or contact with a suspect using alias account information without the authorization of the Chief, Bureau of Organized Crime, or designee.</u>

NOTE: <u>Prior authorization to access information on publicly available internet sources is not required.</u>

4. <u>create an alias account or identity without the authorization of the Chief, Bureau of Organized</u>
Crime or their designee.

(Items indicated by *italics/double underline* were revised.)

Garry F. McCarthy Superintendent of Police

14-081 RWN